CHICAGO
MARCH 4-7

INTERNET2
2024
COMMUNITY
exchange

Managing threats in the quantum soup

Chris Janson, Nokia

March 7, 2024

Discussion topics

1. Quantum computing and R&E networks
2. What’s the downside?
3. ABC’s of cryptography
4. A way forward for R&E networks

Let’s make sense of the soup!

Quantum computers:

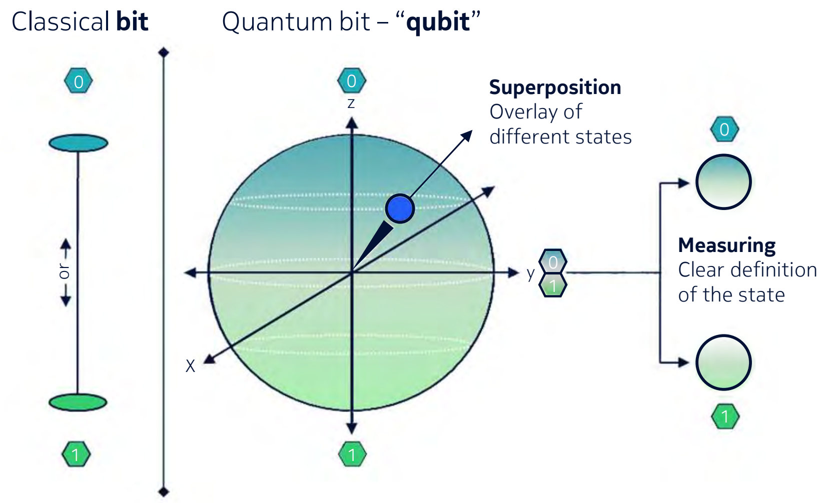
How real are they?
What’s the downside?

Quantum computing

Massively different, massively powerful

- **Quantum computer**: a machine that can perform quantum computations using particles subject to quantum physics– eg: photons or superconducting materials to create logical gates

- **Qubits**: fundamental unit of computation. Allows multiple states at once (superposition) and correlation (entanglement)



Classical **bit**

Quantum bit – “**qubit**”

Superposition
Overlay of
different states

Measuring
Clear definition
of the state

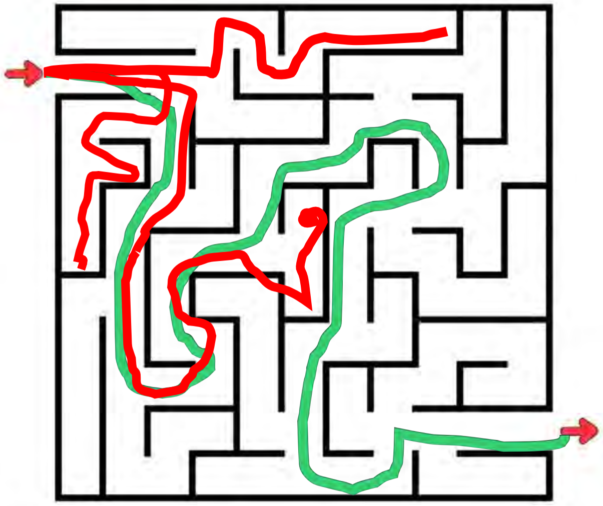
Source: IBM presentation at Quantum World Congress, Sept. ‘23, Washington, DC

Quantum computing

Massively different, massively powerful

Parallel processing at exponential scale:

M. Kaku describes it as capable of finding the path out of a maze in a single path calculation



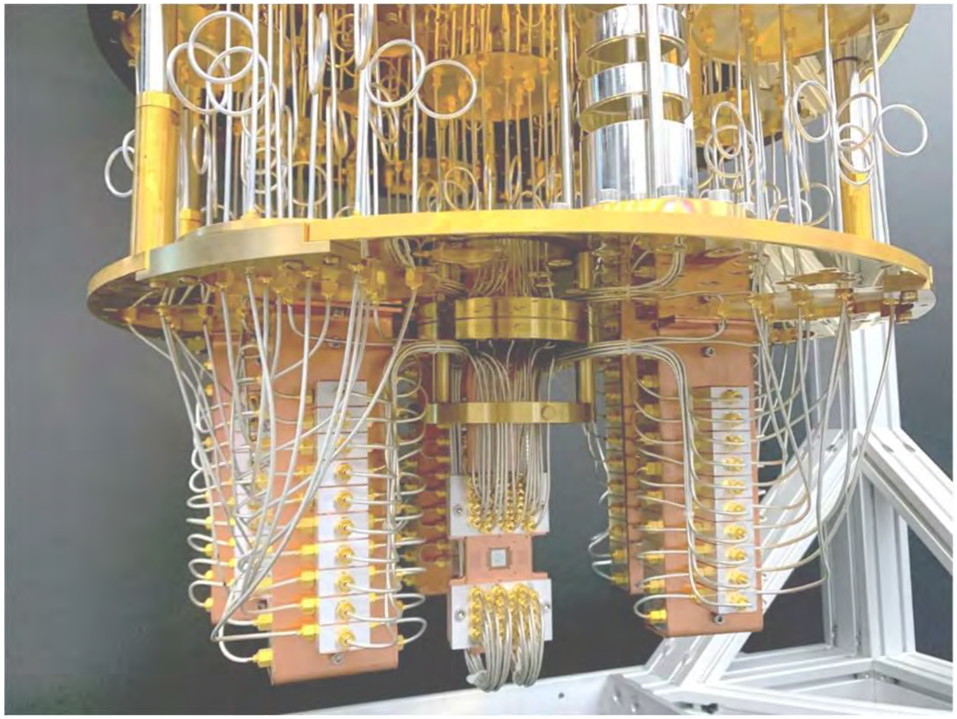
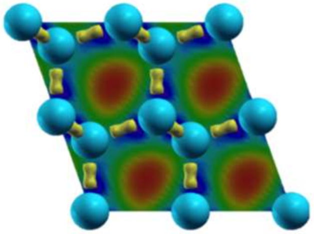


Photo journey inside an IBM quantum computer

Quantum computing

What’s driving their development?

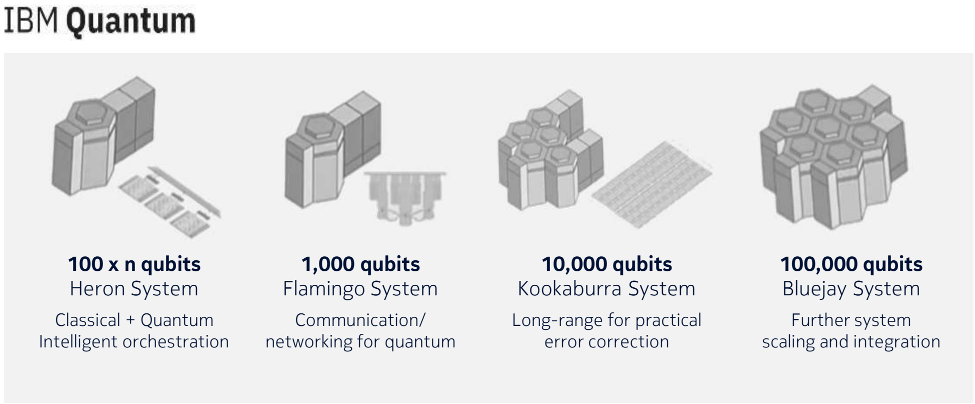
- **Computational speed:** exponential increase
- **Complex problems:** materials research, drug discovery, energy optimization, AI
- **Basic research** and curiosity
- **Information security**



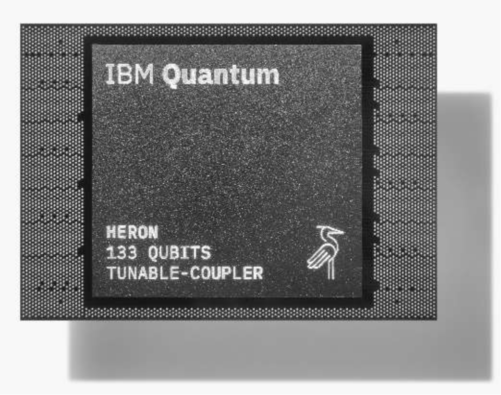
Quantum computing

How real are they? Not just a science project anymore

- **Many technical barriers**: qubit stability, error correction, scaling, supercooling
- **$B’s invested** over past few years, globally; public and private funding
- **Clear progress** reported in multiple papers at SC23
- **IBM announced their System 2**, modular quantum architecture in Dec ’23
  - Roadmap to a 100K Qubit system


IBM Quantum
100 x n qubits
Heron System
Classical + Quantum Intelligent orchestration
1,000 qubits
Flamingo System
Communication/ networking for quantum
10,000 qubits
Kookaburra System
Long-range for practical error correction
100,000 qubits
Bluejay System
Further system scaling and integration

Source: IBM presentation at Quantum World Congress, Sept. ‘23, Washington, DC

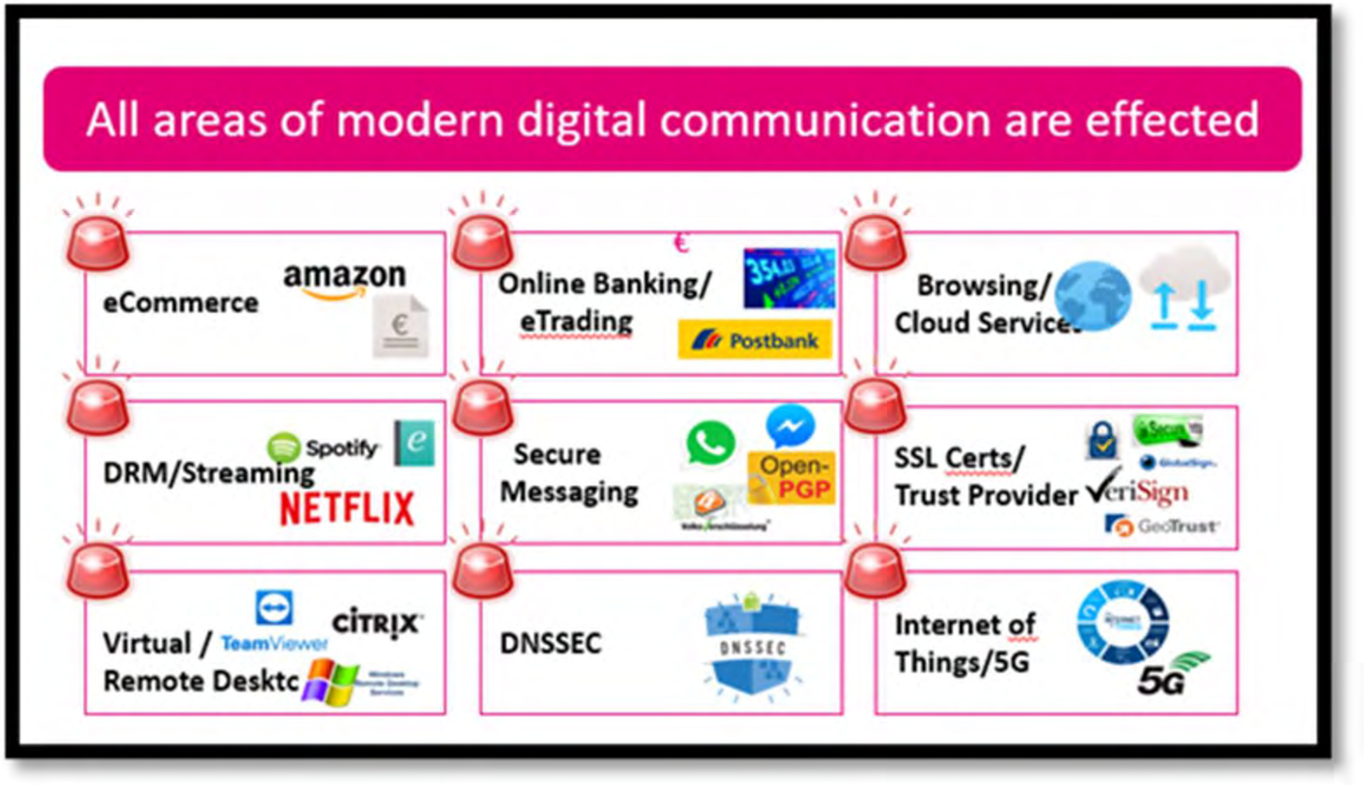


What’s the downside?

Quantum computing breaks a decades-long approach to network security.

All areas of digital communications are affected

A reality that we cannot ignore



All areas of modern digital communication are effected

eCommerce

Online Banking/ eTrading

Browsing/ Cloud Service

DRM/Streaming

Secure Messaging

SSL Certs/ Trust Provider

Virtual / Remote Desktc

DNSSEC

Internet of Things/5G

amazon
€
Postbank
Spotify
NETFLIX
Open-PGP
VeriSign
GeoTrust
TeamViewer
citrix
DNSSEC
5G

Governments responding to increasing Cyberattacks

WORLD ECONOMIC FORUM

CYBERSECURITY

Is your cybersecurity ready to take the quantum leap?

Singapore to build National Quantum-Safe Network that provides robust cybersecurity for critical infrastructure

South Korea plans large scale quantum cryptography adoption

EU urged to prepare for quantum cyberattacks with coordinated action plan

News

Jul 17, 2023 • 5 mins

Cyberattacks Encryption

EPC EUROPEAN POLICY CENTRE

The US is worried that hackers are stealing data today so quantum computers can crack it in a decade

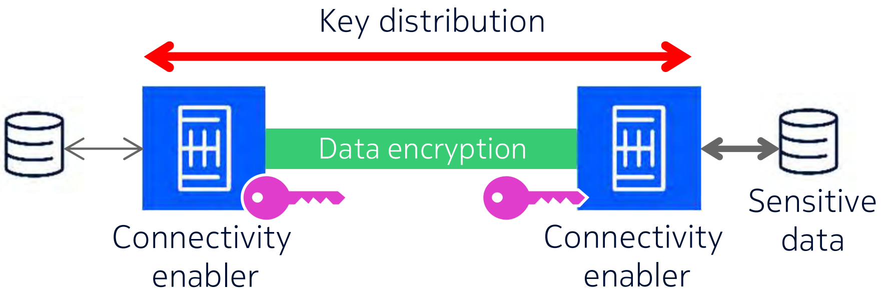
The US government is starting a generation-long battle against the threat next-generation computers pose to encryption.

Quantum Computing

What's the downside?

~~Asymmetric crypto (PKI, DH, ECDH, etc.)~~

Broken

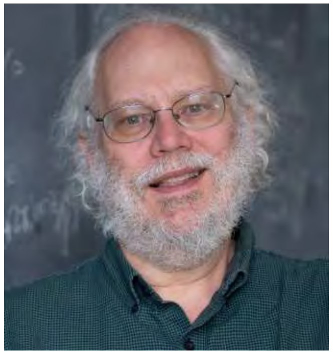


Symmetric crypto

✓

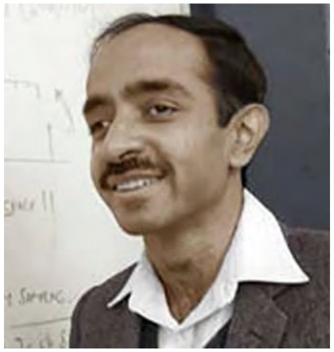
Key effectiveness reduced by 50%.

AES-256 deemed safe



Peter Shor

Algorithm for prime factorization of large integers



Luv Kumar Grover

Shows how to search in √N

First, let's consider some network security basics....

Cryptography is a powerful tool to contain these risks

Integrity
Availability
Information Security
Confidentiality

Eavesdropping

Collect sensitive data, system commands and login info

Confidentiality breached

Man-in-the-middle

Command spoofing with inverted logic of system configuration

Integrity compromised

Denial of service

Flood with illicit control traffic with legitimate IP and TCP/UDP header to overwhelm the system

Availability down

Confidentiality, integrity and availability

Threatened by quantum computing

Integrity
Availability
Information Security
Confidentiality

Eavesdropping

Collect sensitive operational data including system commands and system login info

Confidentiality breached

Man-in-the-middle

Command spoofing with inverted logic (e.g. from close position to open) of system configuration

Integrity compromised

Denial of service

Flood with illicit control traffic with legitimate IP and TCP/UDP header to overwhelm the system

Availability down

Why act now?

CRQC and the HNDL threat

A Quantum computer with a sufficient number of qubits is defined as a **Cryptographically Relevant Quantum Computer (CRQC)** and can decrypt asymmetric security protocols

Harvest Now, Decrypt Later (HNDL)
a clear and present danger

OK, OK ….there's a threat!

What can we do about it?
How hard is this going to be?

Soup's up!: ABC's of cryptography

Integrity
Availability
Information Security
Confidentiality

Public key crypto

DHKE, ECCA, RSA

Asymmetric, public key (PKI) paired with math calculation

Pre-shared key crypto

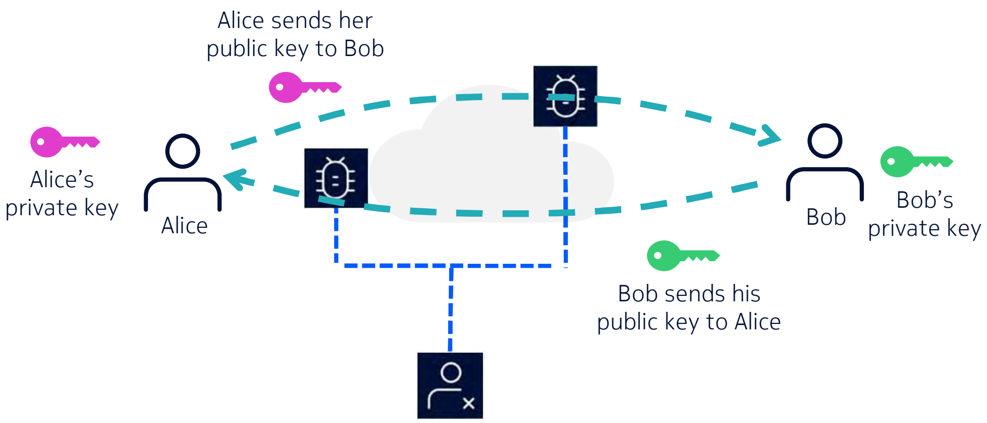
3DES, AES 128/256

Symmetric, pre-shared key (PSK)

Public key cryptography

Public key to encrypt, private key to decrypt

Alice and Bob share their public keys



Alice sends her public key to Bob

Alice's private key

Alice

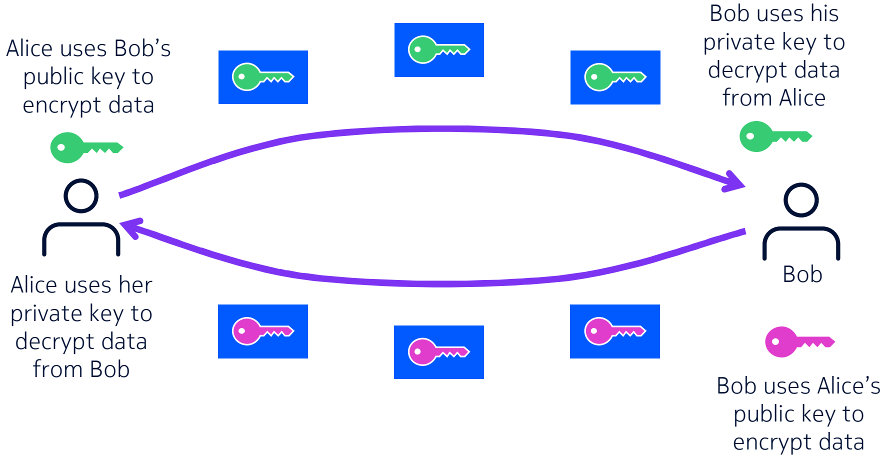
Bob

Bob's private key

Bob sends his public key to Alice

VULNERABILITY:
Eavesdropping was harmless, until now

Alice and Bob send encrypted data using each other's public keys



Alice uses Bob's public key to encrypt data

Alice uses her private key to decrypt data from Bob

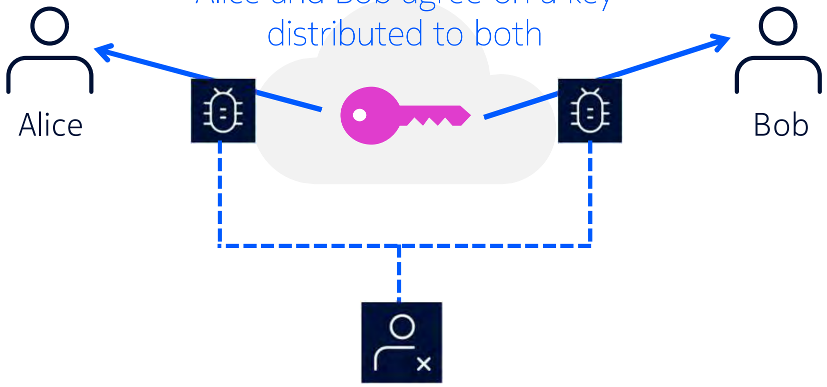
Bob uses his private key to decrypt data from Alice

Bob

Bob uses Alice's public key to encrypt data

Symmetric key cryptography

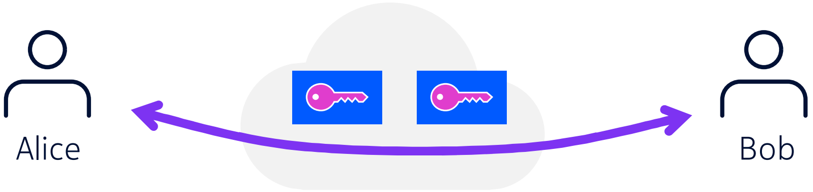
Using one secret key to encrypt to decrypt



Alice and Bob agree on a key distributed to both

VULNERABILITY:
Eavesdropping during key distribution- but safe if key is removed from data path

After receiving the key, they start exchange encrypted data



The ABC's of Cryptography

Essential components

1. Keys

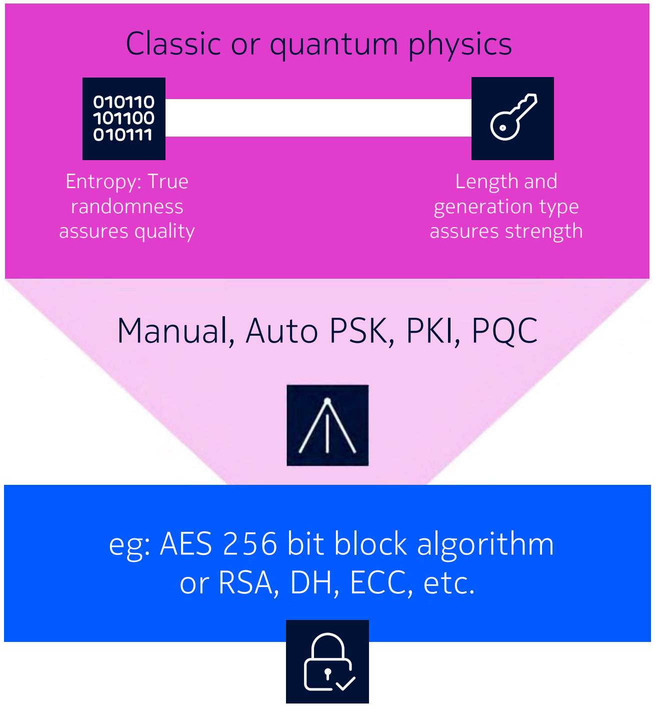
(Quality, Strength)

2. Distribution

(How does the key reach each end?)

3. Locks

(Crypto engine)



Classic or quantum physics

Entropy: True randomness assures quality

Length and generation type assures strength

Manual, Auto PSK, PKI, PQC

eg: AES 256 bit block algorithm or RSA, DH, ECC, etc.

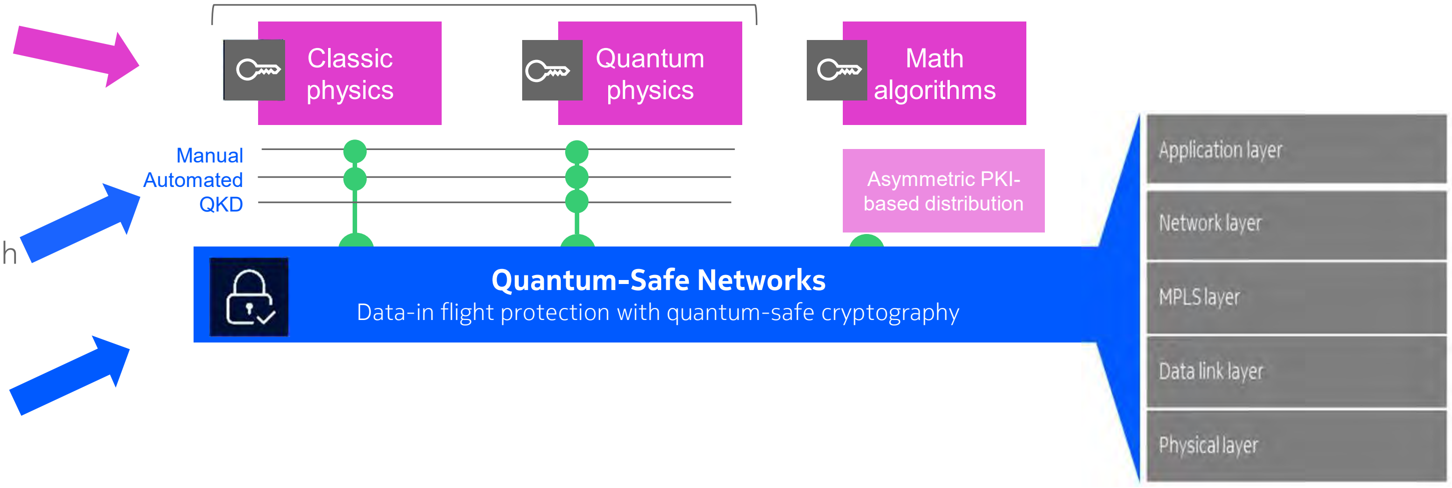
The ABC’s of Cryptography

Key generation & distribution

1. Keys
(Quality, Strength)

2. Distribution
(How does the key reach each end?)

3. Locks
(Crypto engine)



Classic physics

Quantum physics

Math algorithms

Manual
Automated
QKD

Asymmetric PKI-based distribution

Quantum-Safe Networks
Data-in flight protection with quantum-safe cryptography

Application layer

Network layer

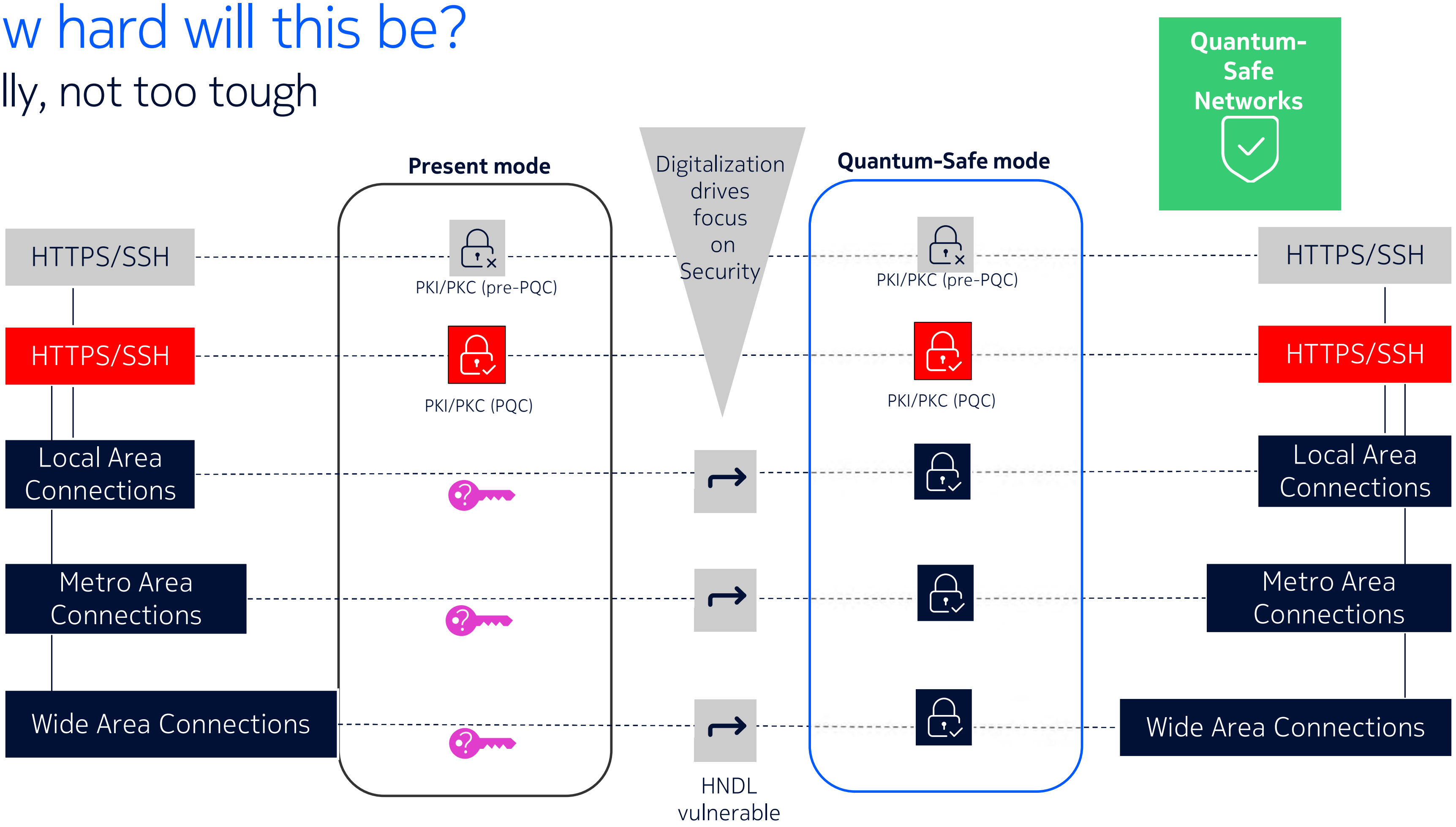
MPLS layer

Data link layer

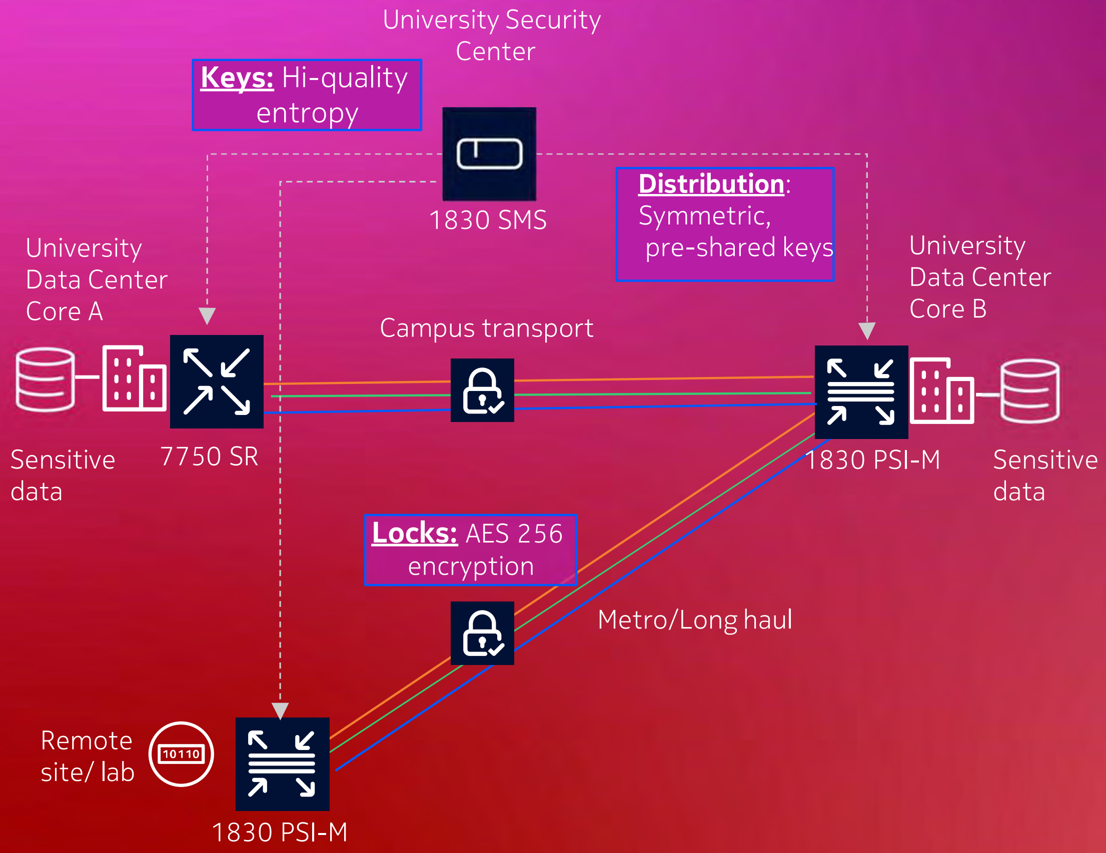
Physical layer

How hard will this be?

Really, not too tough



Quantum-Safe R&E Networks
Multi-layer, adaptable connectivity



University Security Center
Keys: Hi-quality entropy
1830 SMS
Distribution: Symmetric, pre-shared keys
University Data Center Core A
University Data Center Core B
Campus transport
Sensitive data
7750 SR
1830 PSI-M
Sensitive data
Locks: AES 256 encryption
Metro/Long haul
Remote site/ lab
10110
1830 PSI-M

- **Nokia Quantum-Safe network solution:** petabytes of data over campus or long distances (up to 1.2Tbps over 2000 km)
- **Quantum-Safe encryption**: High quality entropy, symmetric, automated pre-shared distribution
- **Defense in depth:** Multiple barriers to attack
- **Protects against HDNL:** Neutralizes immediate threat
- **Long-term protection:** evolves with emerging protection such as QKD and PQC
- **Independent certification:** NIST, Common Criteria, ANSSI

Respond to the threat:

You need to act now

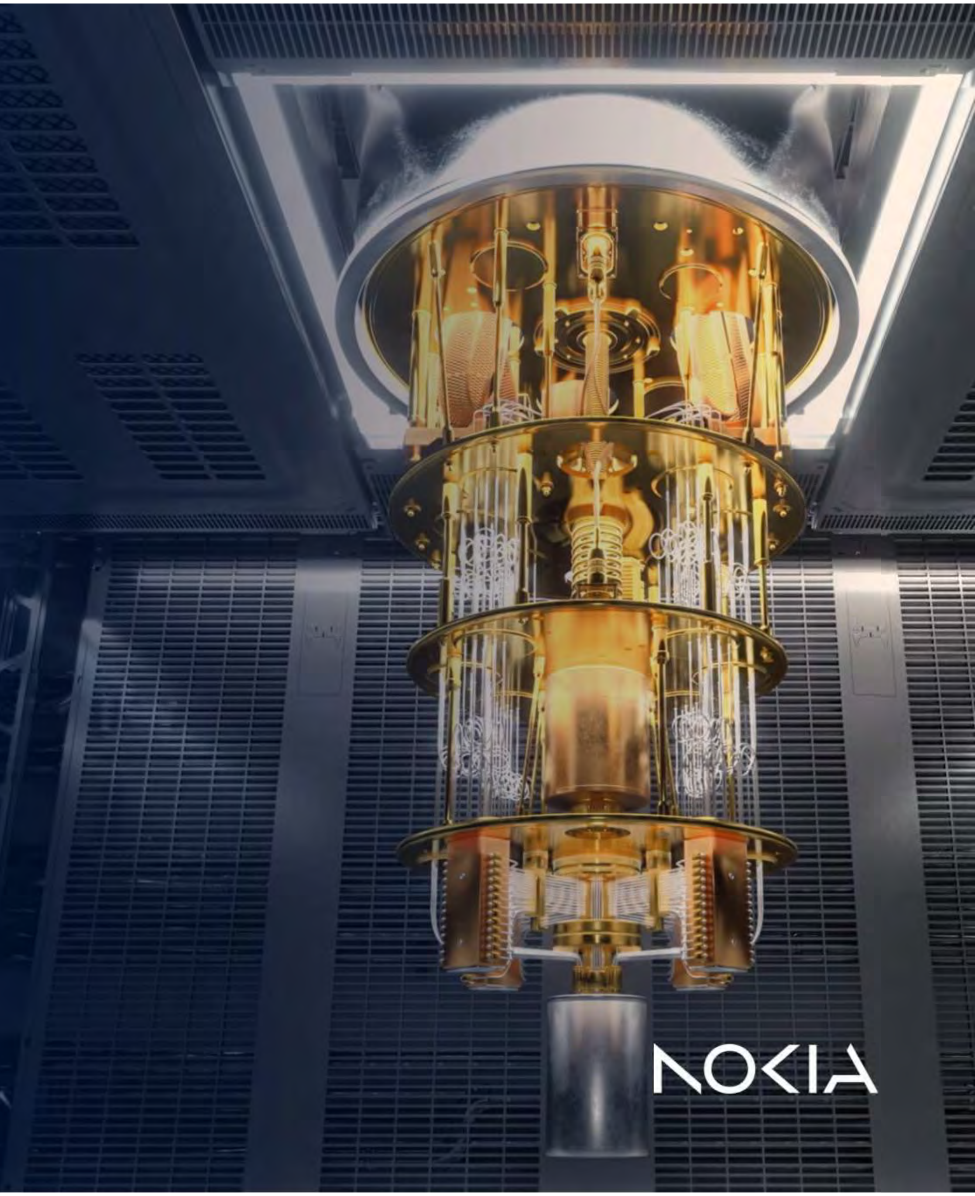
Impossible to "time the threat"

- 5 or 15 years until Q-day? We won't know

New ciphers, new commercial products, system change-outs: all take time. Operators need to plan now and deploy over time

Harvest Now – Decrypt Later

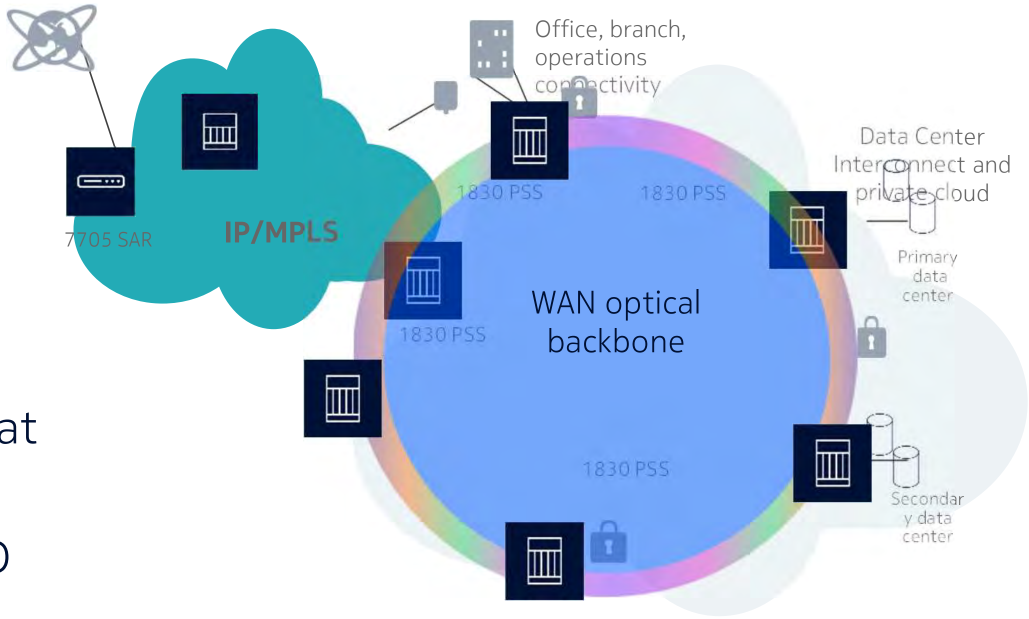
- The present threat is somebody collects and stores your data for later decryption

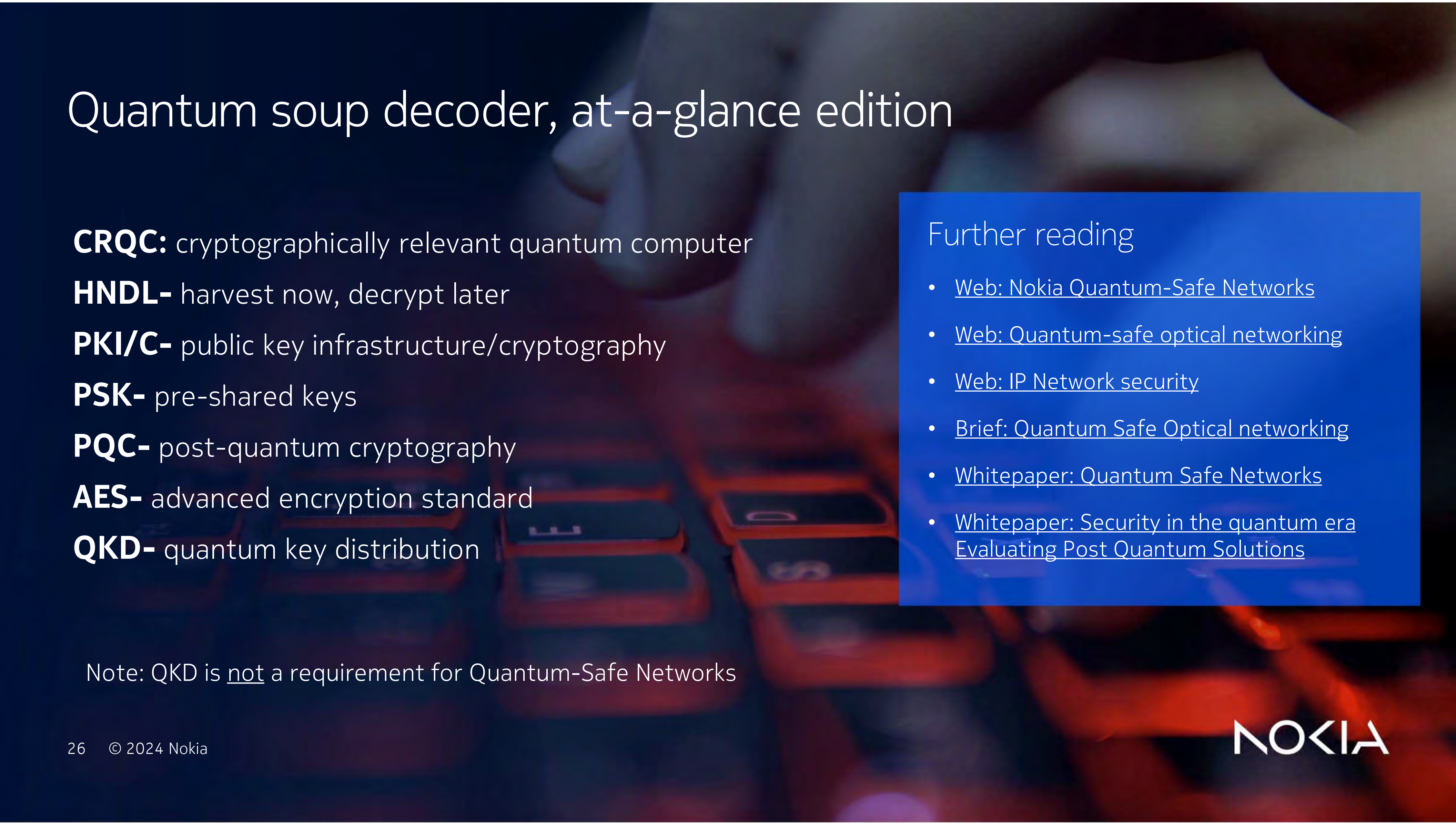


Develop a quantum-readiness roadmap

Recommendations

1. Identify your most vulnerable network connections, nodes or links
2. Ensure deployment of symmetric key distribution today- with classic or quantum entropy sources
3. Update over time, adding protections at additional layers, across the network
4. Watch for critical developments in QKD and PQC– be ready for future further actions





Quantum soup decoder, at-a-glance edition

CRQC: cryptographically relevant quantum computer

HNDL- harvest now, decrypt later

PKI/C- public key infrastructure/cryptography

PSK- pre-shared keys

PQC- post-quantum cryptography

AES- advanced encryption standard

QKD- quantum key distribution

Further reading

- Web: Nokia Quantum-Safe Networks
- Web: Quantum-safe optical networking
- Web: IP Network security
- Brief: Quantum Safe Optical networking
- Whitepaper: Quantum Safe Networks
- Whitepaper: Security in the quantum era Evaluating Post Quantum Solutions

Note: QKD is not a requirement for Quantum-Safe Networks

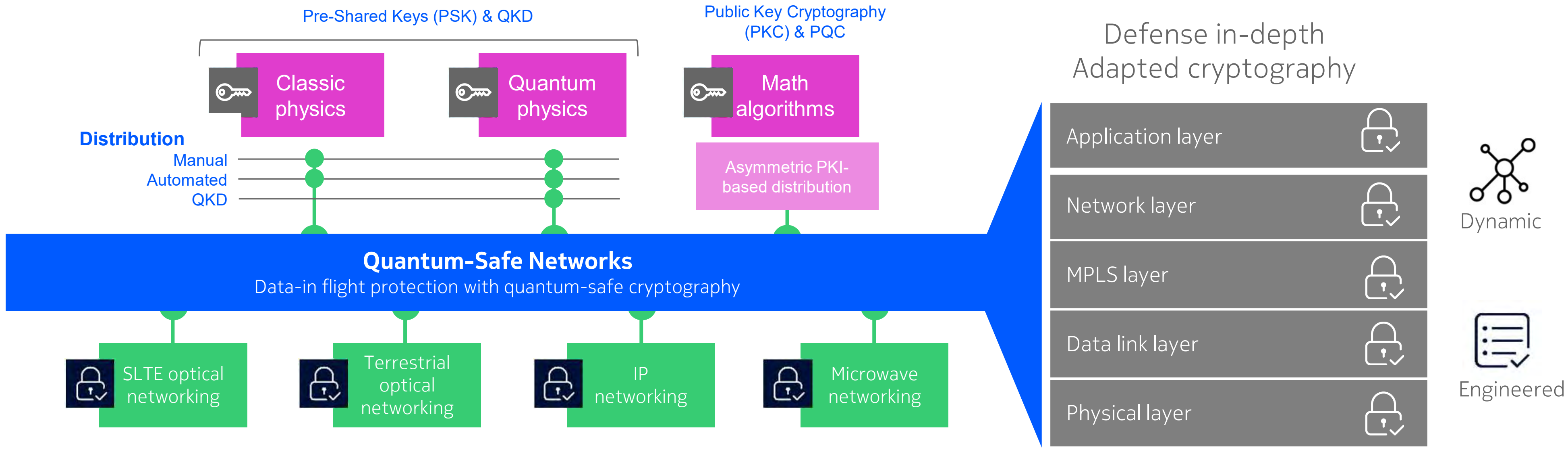
Questions?

NOKIA

Backup slides

Quantum-safe networks

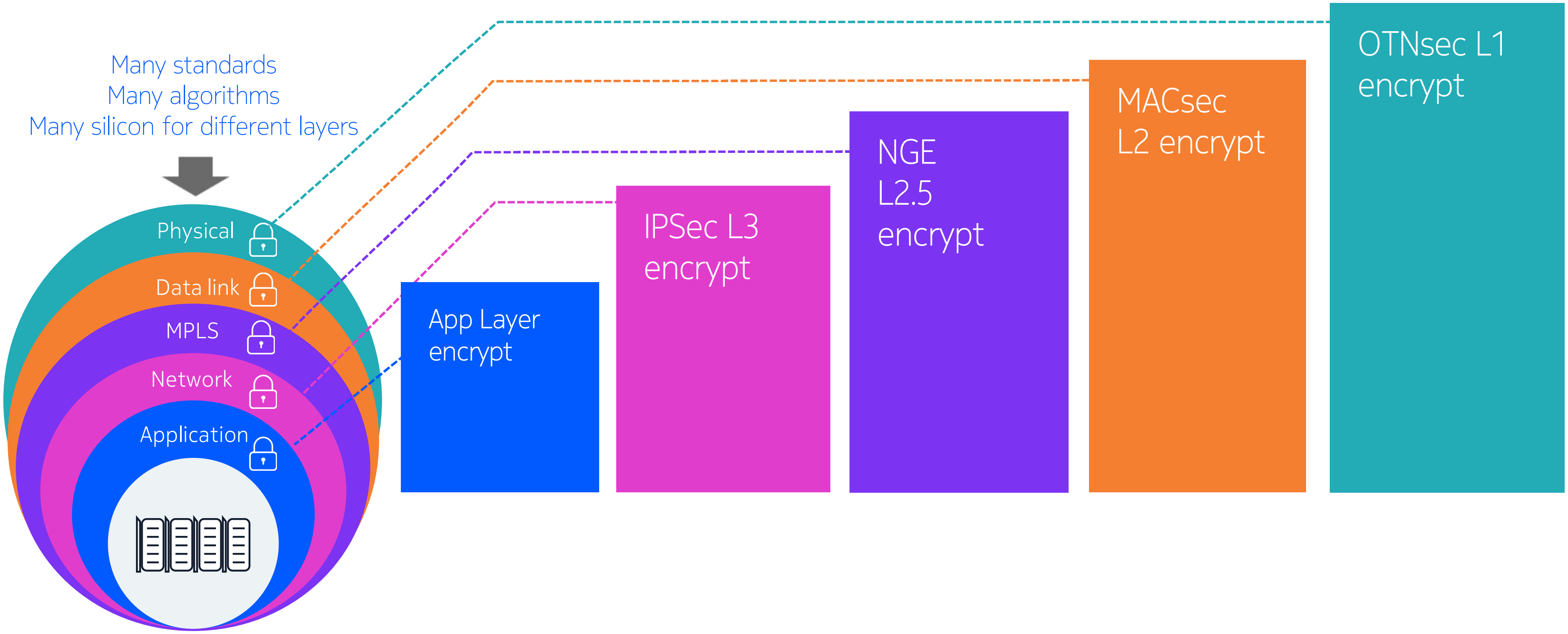
Multi-domain transport solution for data in-flight protection



Complementary today and tomorrow Quantum-Safe cryptography creating the backbone of Quantum-Safe communication

Act now

Multi-layer defense-in-depth

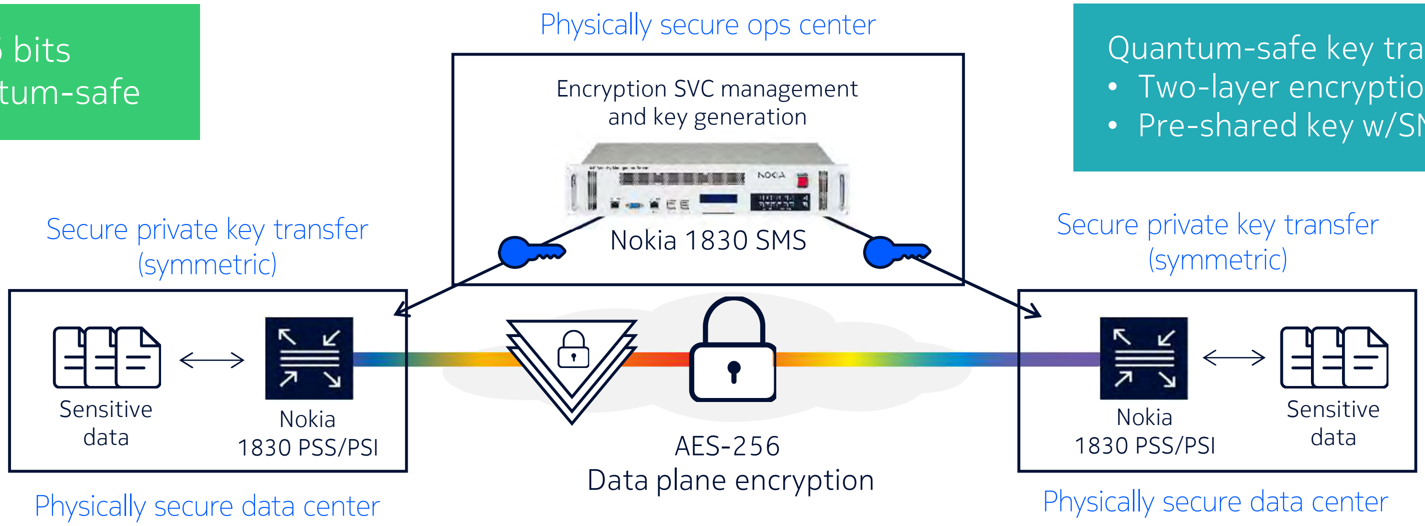


Nokia Quantum-Safe Networks: optical layer

Pre-shared-key management

All links ensure 256 bits key strength: quantum-safe

Quantum-safe key transport:
- Two-layer encryption
- Pre-shared key w/SNMPv3



Physically secure ops center

Encryption SVC management and key generation

Nokia 1830 SMS

Secure private key transfer (symmetric)

Secure private key transfer (symmetric)

Sensitive data

Nokia 1830 PSS/PSI

AES-256 Data plane encryption

Nokia 1830 PSS/PSI

Sensitive data

Physically secure data center

Physically secure data center

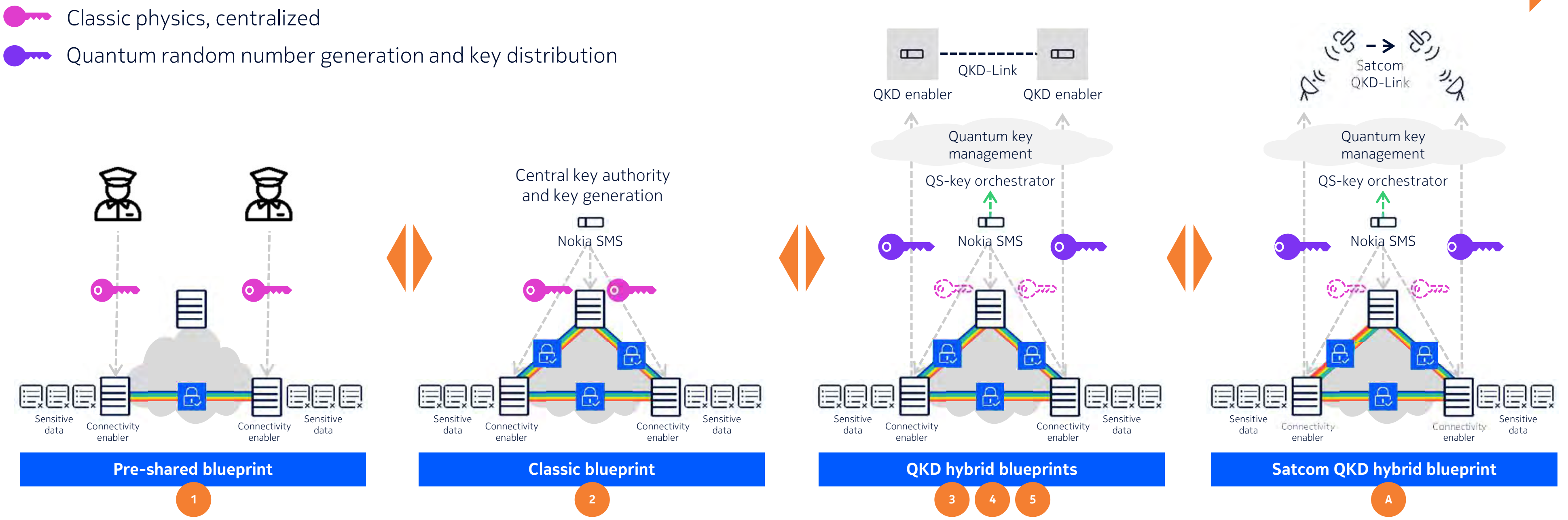
Quantum-safe data transport:
- Data plane fiber taps contain only ciphertext
- Optical overhead does not contain key agreement

Quantum-safe data transport:
- Symmetric, AES-256
- No key exchange on fiber link

Quantum-Safe Network evolution

Example of PSK evolution

Your Quantum-Safe roadmap: Begin today and adapt to tomorrow's innovations



Classic physics, centralized

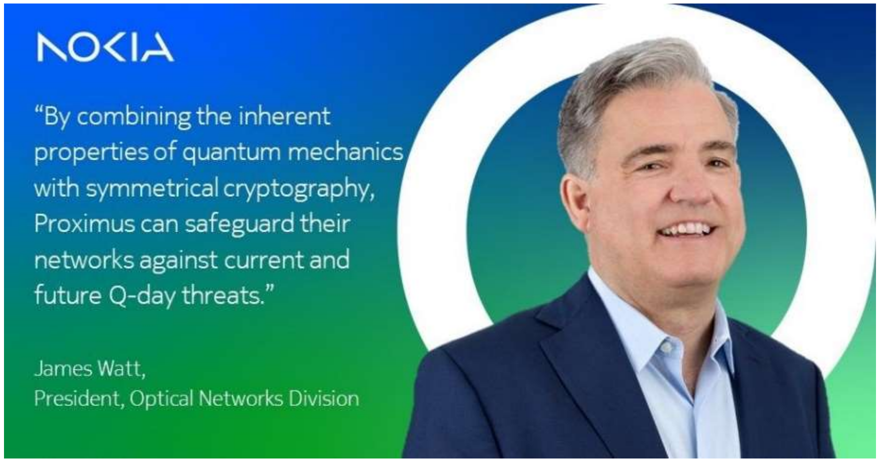
Quantum random number generation and key distribution

Public references

Europe’s first live hybrid quantum encryption key trial

Trial demonstrates first use of hybrid encryption method in a live network – highlights use of both classic and quantum physics methods to symmetrically generate and distribute out-of-band keys allowing for the delivery of quantum-safe cryptography services

Official Press Release



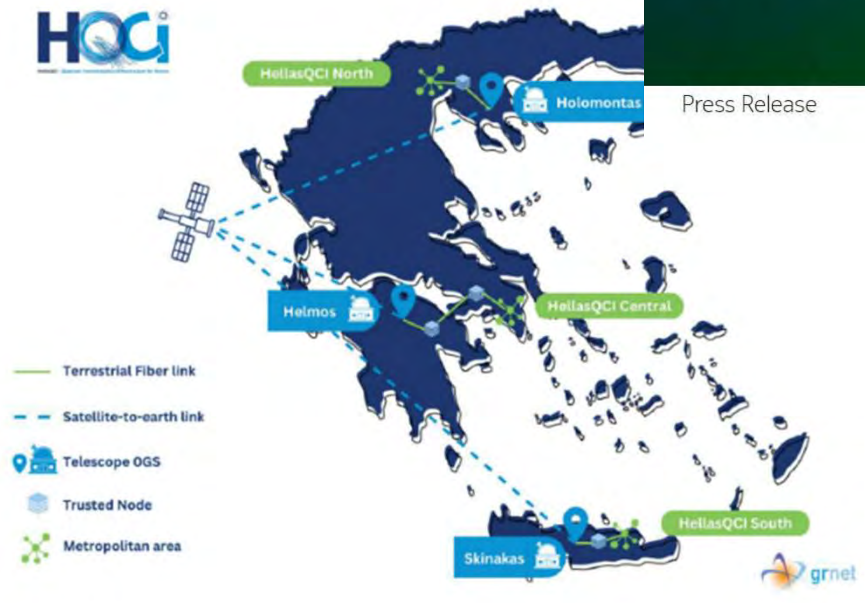
“By combining the inherent properties of quantum mechanics with symmetrical cryptography, Proximus can safeguard their networks against current and future Q-day threats.”

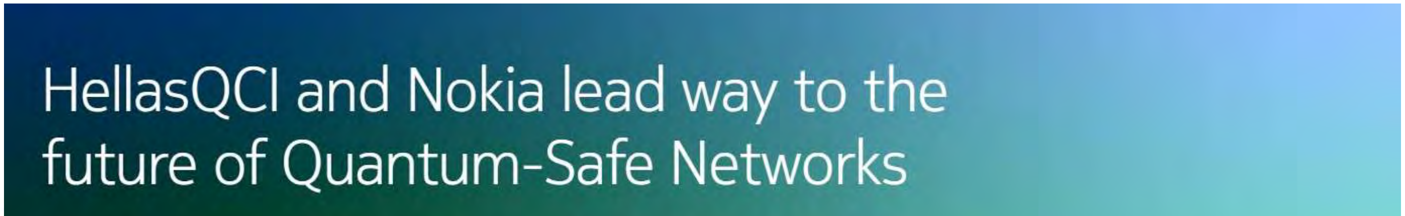
James Watt,
President, Optical Networks Division

Enabling quantum security in (optical) networks

Public references

QKD trial in Greece




HellasQCI and Nokia lead way to the future of Quantum-Safe Networks

Press Release

Dr. Ognjen Prnjat, Director for European Infrastructures and Projects Directorate at GRNET, said: “We are very pleased with the successful completion of the PoC with Nokia, which is one of the key milestones for the HellasQCI project..”

Random Number Generators

SROS

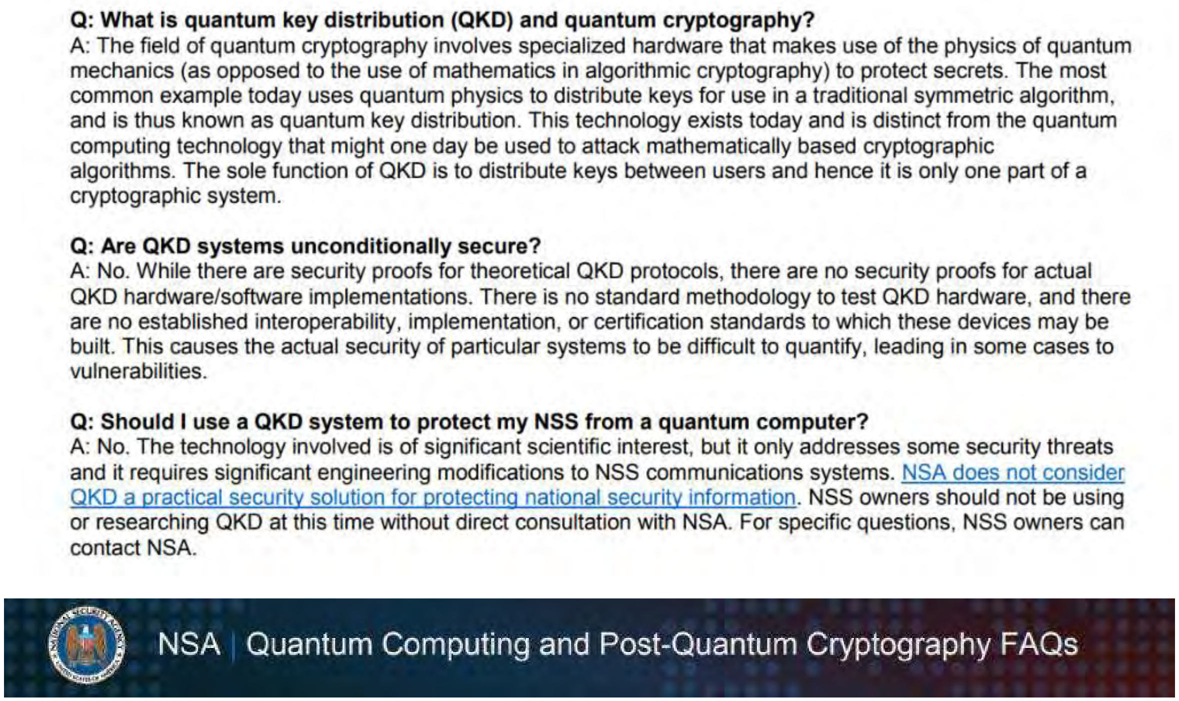
Key quality depends on key generation, especially in random number generation and the seed used to create that random number

- Pseudo-Random Number Generation (P-RNG)
- Classic Physics-based Random Number Generation (CP-RNG)
- Quantum Random Number Generation (Q-RNG)

SROS uses a classical RNG and generates keys with an entropy of 512 bits

QKD is an emerging part of future post-quantum architectures

According to the NSA



Q: What is quantum key distribution (QKD) and quantum cryptography?
A: The field of quantum cryptography involves specialized hardware that makes use of the physics of quantum mechanics (as opposed to the use of mathematics in algorithmic cryptography) to protect secrets. The most common example today uses quantum physics to distribute keys for use in a traditional symmetric algorithm, and is thus known as quantum key distribution. This technology exists today and is distinct from the quantum computing technology that might one day be used to attack mathematically based cryptographic algorithms. The sole function of QKD is to distribute keys between users and hence it is only one part of a cryptographic system.

Q: Are QKD systems unconditionally secure?
A: No. While there are security proofs for theoretical QKD protocols, there are no security proofs for actual QKD hardware/software implementations. There is no standard methodology to test QKD hardware, and there are no established interoperability, implementation, or certification standards to which these devices may be built. This causes the actual security of particular systems to be difficult to quantify, leading in some cases to vulnerabilities.

Q: Should I use a QKD system to protect my NSS from a quantum computer?
A: No. The technology involved is of significant scientific interest, but it only addresses some security threats and it requires significant engineering modifications to NSS communications systems. NSA does not consider QKD a practical security solution for protecting national security information. NSS owners should not be using or researching QKD at this time without direct consultation with NSA. For specific questions, NSS owners can contact NSA.

NSA | Quantum Computing and Post-Quantum Cryptography FAQs